УДК 004
ББК 32.81

МНОГОАГЕНТНАЯ ЭВОЛЮЦИОНИРУЮЩАЯ СИСТЕМА КАК СРЕДСТВО КОНТРОЛЯ НАД ВНУТРЕННИМИ ЗЛОУМЫШЛЕННИКАМИ

А.А. Бешта

В данной статье информационная система представлена в качестве неоднородной и непостоянной структуры. Рассмотрены характеристики внутреннего злоумышленника. Обоснована возможность использования многоагентных технологий для контроля над внутренним злоумышленником. Рассмотрены механизмы эволюции популяции агентов.

Ключевые слова: *многоагентная система, генетические алгоритмы, внутренний злоумышленник, информационная система, эволюция агента.*

В настоящее время происходит развитие многоагентных технологий при решении вопросов защиты информации. Компания Symantec давно производит свой продукт Enterprise Security Manager, в котором заявлено использование многоагентных технологий. В научных кругах также этот вопрос не оставлен без внимания, и многие исследуют применение агентов к защите информации [3]. Однако можно обозначить узкую направленность этих исследований. Большинство авторов ограничиваются рассмотрением внешнего злоумышленника или их группы, пытающихся реализовать DDOS атаку на информационную систему [2].

Следует отметить, что по статистике наибольшую опасность представляет внутренний злоумышленник, который – умышленно или нет – может нанести ущерб организации.

Существует много средств, защищающих от внутреннего злоумышленника. Они обеспечивают разграничение доступа, контроль действий сотрудников, то есть загоняют пользователей в жесткие рамки. Но организация в целом и информационная система как ее часть – динамическая структура, взаимодействующая с окружающим миром. А окружающей среде свойственна неопределенность.

Кроме того, сама информационная система состоит из взаимодействующих, изменяющихся во времени элементов: средства вычислительной техники, каналы связи, данные, люди. Всем коллективам свойственно особое социальное поведение. Они взаимодействуют между собой для достижения цели, общаются, оценивают и так далее. И этого нельзя не учитывать при решении вопросов защиты информации.

Можно выделить следующие особенности информационных систем:

- неопределенность в поведении внешней среды;
- непостоянство во времени;
- множество разнородных объектов и компонентов;
- социальное взаимодействие.

Внутренний злоумышленник имеет доступ к информационной системе изнутри организации. Уровни доступа следующие:

- полный доступ к информационной системе (администраторы);
- пользовательский доступ к информационной системе (сотрудники);
- доступ к технической документации (технический персонал);
- доступ к оборудованию (вспомогательный персонал).

Кроме того, злоумышленник имеет доступ в организацию и, следовательно, имеет возможность установки дополнительных средств вычислительной техники, сетевого оборудования. То есть он может изменить топологию сети и состав информационной системы с целью обхода защитных механизмов.

Цели злоумышленника по отношению к информационным ресурсам зависят от их побуждений:

- хищение или копирование информации (чтобы передать / продать ее конкурентам);
- ознакомление с информацией (чтобы получить собственную выгоду);
- уничтожение или модификация информации (чтобы нарушить работоспособность системы).

Также можно выделить два типа условий совершения злоумышленных действий. В первом случае сотруднику случайно предоставляется возможность совершить это действие и получить какую-то выгоду. Его действия имеют спонтанный характер, не запланированы и не подготовлены.

Во втором случае действия спланированы и подготовлены. Злоумышленников может быть несколько, и они могут действовать организованной координируемой группой.

Таким образом, можно выделить следующие особенности в описании внутреннего злоумышленника:

- возможность анализа информационной системы;
- возможность нарушения структурной и функциональной целостности информационной системы;
- возможность планирования и координации действий;
- получение выгоды при совершении злоумышленных действий.

Таким образом, имеется необходимость в разработке инструмента, позволяющего выявлять спланированные и координируемые воздействия на информационную систему внутренним злоумышленником и предупреждать эти воздействия или снижать потенциальный ущерб до приемлемого уровня. Такая система должна учитывать возможность анализа информационной системы и изменения ее структурной и функциональной целостности и принимать во внимание ее неоднородность и непостоянность во времени и неопределенность окружающей среды.

При моделировании различных отношений в последнее время широко используются многоагентные технологии. Этот подход позволяет представить некоторую область в виде группы независимых агентов, действующих совместно для достижения некоторой цели.

Агент представляет собой независимую программную сущность, функционирующую в некоторой среде, способную к самостоятельным действиям в этой среде с целью достижения поставленной цели. Агент имеет свое представление об окружающей среде и реагирует на их изменение. Формально агента можно представить в виде кортежа:

$$Agent = <Pr, Act, Know, Goal>, \quad (1)$$

где Pr – свойства агента,
Act – набор действий агента;
$Know$ – набор знаний агента;
$Goal$ – цели агента.

При достижении поставленной цели агент руководствуется не только собственными знаниями и опытом, но также может взаимодействовать с другими агентами.

Таким образом, можно образовать группу агентов, взаимодействующих между собой для достижения общей цели. Такой подход позволяет моделировать социальные отношения коллектива, когда несколько человек с различным опытом и знаниями пытаются достичь некоторого результата.

Основой для работы агента служат его знания. Для разработки многоагентной системы необходимо определить предметную область, в которой будут существовать агенты, и наполнить ее необходимой информацией. Для системы контроля над внутренним злоумышленником важнейшей составляющей являются знания об информационной системе, в которой будут функционировать агенты.

Для представления знаний используется онтология [1].

Онтология представляет собой формальное описание некоторой области знаний в виде набора понятий и отношений между этими понятиями.

Обобщенно онтологию можно представить в следующем виде:

$$O = \{E^O, Rel^O\}, \quad (2)$$

где E^O – *множество* классов элементов информационной системы, $E_j^O, j = \overline{1,J}, j \in N$;

Rel^O – множество отношений между элементами информационной системы, $Rel^O \subseteq E^O \times E^O$.

Каждый класс E_j^O представляет собой совокупность однотипных сущностей, описанных с помощью набора свойств:

$$E_j^O = \{P_{jk}^O\}, \quad (3)$$

где P_{jk}^O – свойство класса E_j^O.

При этом следует учитывать, что свойство класса может быть объектом другого класса и описываться своими свойствами.

Отношения между элементами Rel^O представляются следующим образом:

$$Rel^O = Rel_{is}^O \cup Rel_{part}^O, Rel_{is}^O \cap Rel_{part}^O = \varnothing, \quad (4)$$

где Rel_{is}^O – отношение категоризации между элементами;

Rel_{part}^O – отношение принадлежности между элементами.

Данная онтология представляет собой обобщенное описание информационной системы. В ней описываются все возможные элементы и их свойства.

При создании онтологии информационной системы контроля над внутренним злоумышленником в множество элементов E^S включают подмножества элементов особых типов:

- множество узлов ВС $E_H^S, E_H^S \subseteq E^S$;
- множество компонентов ВС $E_C^S, E_C^S \subseteq E^S$;
- множество уязвимостей элементов ВС $E_V^S, E_V^S \subseteq E^S$;
- множество активов ВС $E_A^S, E_A^S \subseteq E^S$;
- множество средств защиты ВС $E_{SP}^S, E_{SP}^S \subseteq E^S$;
- множество связей $E_L^S, E_L^S \subseteq E^S$;
- множество пользователей $E_U^S, E_U^S \subseteq E^S$;
- множество разрешений $E_P^S, E_P^S \subseteq E^S$.

Это позволяет описывать множество компонентов информационной системы, активы и информационные и физические связи.

Особенность многоагентной системы в ее распределенности и децентрализованности. Агент функционирует в рамках узла или сегмента информационной системы. Это означает, что каждый агент обладает частью информации. Многоагентный подход позволяет преодолеть неполноценность и некоторую неопределенность информации о среде для отдельного агента. Это достигается путем взаимодействия с другими агентами, они могут обмениваться информацией.

Для построенной модели информационной системы E^S каждый агент вычисляет защищенность, то есть свою функцию полезности $P = f(E^S) = f(E_j^S) = f(P_{jk}^S)$, j $\in$ {*H, C, V, A, SP, L, U, P*} для заданного сегмента, зависящую от свойств элементов информационной системы. Перед системой стоит задача найти оптимальное распределение значений свойств элементов информационной системы $P' = \text{opt } f(P_{jk}^S)$, при котором функция полезности достигает заранее установленного значения. Решение задачи поисковой оптимизации на многомерном пространстве решений достигается применением генетических алгоритмов. Появление новых агентов обеспечивается следующими биологическими механизмами: селекцией, скрещиванием, мутацией.

Оператор скрещивания создает одного или нескольких потомков. Генерируется новый вектор параметров функции полезности агента, находящийся в окрестности родительских векторов.

Пусть $C_1 = (c_1^1, c_2^1, \ldots, c_n^1)$ и $C_2 = (c_1^2, c_2^2, \ldots, c_n^2)$ – хромосомы (вектора параметров) двух агентов, выбранных оператором селекции для скрещивания. В результате скрещивания создается потомок $H_1 = (h_1^1, \ldots, h_n^1)$, где $h_k^1 = f(c_k^1, c_k^2)$, $k = 1, \ldots, n$. В качестве функции скрещивания используется *SBX*-кроссовер, имитирующий двоичный. Тогда

$$h_j^1 = 0{,}5[(1 - \beta_k)c_j^1 + (1 + \beta_k)c_j^2], \quad (5)$$

где β_k – число, сгенерировано по формуле:

$$\beta(u) = \begin{cases} (2u)^{\frac{1}{n+1}}, u(0,1) \le 0{,}5 \\ \left(\frac{1}{2(1-u)}\right)^{\frac{1}{n+1}}, u(0,1) > 0{,}5 \end{cases}. \quad (6)$$

В формуле $u(0,1)$ – случайное число, распределенное по равномерному закону, n – параметр кроссовера.

После скрещивания производится механизм мутации. То есть каждое значение вектора с некоторой вероятностью изменяется на некоторую величину. Для этого используется неравномерная мутация Михалевича:

$$c_i = \begin{cases} c_i + \delta(t, b_i - c_i) & \text{при } \chi = 0 \\ c_i + \delta(t, c_i - a_i) & \text{при } \chi = 1 \end{cases}, \quad (7)$$

$$\delta(t, y) = y\left(1 - r^{\left(1 - \frac{t}{\varepsilon_{max}}\right)^b}\right) \quad (8)$$

где χ – целое случайное число, принимающее значение 0 или 1; $r \in [0,1]$ – случайное вещественное число;

ε_{max} – максимальное количество эпох алгоритма;

b – параметр мутации.

Размер популяции агентов ограничен и при его превышении агенты, имеющие наименьшее значение функции полезности, уничтожаются. Таким образом, постепенно новые агенты с эффективной функцией полезности вытесняют менее эффективных.

В результате этого система оптимизируется к заданным условиям работы и может эффективно контролировать внутреннего злоумышленника во времени.

Работа системы контроля над внутренним злоумышленником в информационной системе на примере разработанной модели будет включать в себя следующие этапы:

1. Создание начальной группы агентов. На этом этапе создается начальная популяция агентов и происходит их распределение по сегментам информационной системы.

2. Сбор исходной информации об информационной системе для построения ее модели. На данном этапе осуществляется сбор информации о компонентах, ресурсах, связях и других элементах, представленных в онтологии.

3. Оценка модели. На данном этапе определяются уровни защищенности сегментов и компонентов информационной системы, выявляются уязвимые места.

4. Моделирование внутреннего злоумышленника. На этом шаге определяются наиболее вероятные действия злоумышленника, сценарий атаки, последствия воздействия.

5. Анализ результатов моделирования. Анализируются результаты действий внутреннего злоумышленника и способность системы выявлять данные воздействия.

6. Модификация популяции агентов. Эволюционное изменение популяции агентов и повторное моделирование. Повторяется, пока не будет достигнута необходимая эффективность группы агентов.

7. Выработка рекомендаций. Делается вывод о способности информационной системы противостоять воздействиям внутреннего злоумышленника и возможных рисках, предлагаются решения по упреждению злоумышленных воздействий.

Таким образом, рассмотренная система способна оптимизироваться к заданным условиям неоднородной и непостоянной окружающей среды и может эффективно контролировать внутреннего злоумышленника во времени. Предложена модель представления информации и механизмы оптимизации многоагентной системы.

СПИСОК ЛИТЕРАТУРЫ

1. Goluch, G. Integration of an Ontological Information Security Concept in Risk Aware Business Process Management / G. Goluch, A. Ekelhart, S. Fenz // Proceedings of the 41st Hawaii International Conference on System Sciences, HICSS2008 / IEEE Computer Society. – Waikoloa, Hawaii, 2008. – P. 377–385.

2. Kotenko, I. Agent-based Simulation Environment and Experiments for Investigation of Internet Attacks and Defense Mechanisms / I. Kotenko, A. Ulanov // Proceedings of 21th European Conference on Modelling and Simulation (ECMS 2007), Prague, 4–6 June 2007. – Prague, 2007. – P. 146–155.

3. Shoham, Y. Multiagent Systems: Algorithmic, Game-Theoretic, and Logical Foundations / Y. Shoham, K. Leyton-Brown. – Cambridge : Cambridge University Press, 2009. – 532 p.

MULTIAGENT EVALUATING SYSTEM AS A MEANS OF CONTROL FOR INVADERS

A.A. Beshta

Information system described like inhomogeneous and non-permanent structure. Considered insiders characteristics. Giving substantiation possibility of multiagent systems using to insider control. Considered mechanisms of agent population evolution.

Key words: *multiagent system, genetic algorithm, insider, information system, agent evolution.*